ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

DISD ACCEPTABLE USE POLICY

The Denton ISD Acceptable use Policy applies to all users of Denton ISD’s Electronic Commu­nications Systems. Users include:

• Denton ISD employees

• Denton ISD students

• Contractors

• Consultants

• Student Teachers

• Temporary workers

• Any third parties that use the system

Student Acceptable Use Policy

DISD is pleased to offer students access to a computer network for file sharing, storage, printing, electronic mail and the Internet while at school. Parents that prefer their child not have computer access should send a request in writing to the campus principal. Educating minors about appro­priate online behavior such as interacting with other individuals on social networking websites, chat rooms and cyber bullying will be addressed by campus DISD staff such as Curriculum Technology Specialists, Technology Integrators, teachers and counselors.

Web Enabled Devices from Home

DISD will grant students in grades 6-12 permission to bring a personal web-enabled device from home to campus for their academic use. Student use of personally-owned devices in the class­room setting will be at the discretion of campus administration and/or classroom teachers.

Students who use web-enabled devices from home will have access to wireless Internet but will not have access to any district drives such as network folders. Network drives can only be ac­cessed via district machines.

Students must check in their device with the Campus Tech as well as give them the administra­tor login to the device. A service tag will be placed on the device to let staff know the device has been checked in.

DISD is not liable for any loss or damage incurred, nor can it load any software onto a student web-enabled device (software & hardware). Students should secure their devices in a locked locker. All students’ laptops and digital devices should be clearly labeled with the student’s name.

Identity theft is a growing problem. We recommend that any personally sensitive files (such as tax documents, social security information, bank records, etc.) are removed from any device before it is used on campus.

Users will not loan their device to someone else. The user is responsible for any content on the device regardless of how it originated.

All technological devices brought onto a DISD campus are subject to search and seizure. Im­proper or non-educational use could result in loss of privileges for the on-campus use of such devices.

108

DISD is not responsible for lost, damaged, or stolen devices.

Any dispute involving Acceptable Use of district or personal resources will be settled at the dis­cretion of District personnel.

What is expected?

The DISD Student Code of Conduct applies to electronic interaction, just as it would in any face to face interaction. Communications on the network are often public in nature. General campus and district rules for behavior and communications apply. It is expected that users will comply with district standards and the specific rules set forth below.

The use of the network is a privilege, not a right, and may be revoked if abused. The user is per­sonally responsible for his/her actions in accessing and utilizing the school's computer resources or personal computer resources used on district property. The students are advised never to ac­cess, keep, or send anything that they would not want their parents, teachers, or administrators to see.

Monitored Use

Electronic mail transmissions and any other use of the electronic communications system by stu­dents are not confidential and may be monitored at any time by designated District staff to ensure appropriate use for educational purposes.

Access to district approved email accounts and the Internet will allow students access to avail­able online textbooks, explore thousands of libraries, databases, museums, and other repositories of information, and to collaborate with other Internet users around the world. The district filters the Internet for objectionable material. However, families should be aware that some material might still contain items that are illegal, defamatory, inaccurate, or potentially offensive. While the purposes of the district are to use Internet resources for constructive, educational goals, students may find ways to access other materials. We believe the educational benefits, access to informational resources, and opportunities for global collaboration exceed the disadvantages. The district considers computer and guided Internet use a part of the instructional program just like a textbook.

Privacy/Security

Network storage areas and school and personal web-enabled devices brought on school prop­erty can be treated like school lockers. Students should never access network accounts, network folders, and files that are not theirs. Students will not circumvent District security measures. DISD may revoke any District user’s access until the violation is reviewed by appropriate district administrators. Network administrators may review communications and content to maintain sys­tem integrity and to ensure that students are using the system responsibly. The user understands and agrees to assume all risks and responsibilities when using their personal devices. The user is responsible for any content on their device, regardless of how it originated.

109

Storage

Users are expected to remain within allocated disk space for all district owned resources. Stu­dents should never download or install any software or applications onto network drives or disks. Any assumed violation will be reported to the appropriate district administrator and the user’s privilege revoked until the concern of violation is reviewed by the appropriate district adminis­trator.

Posting Policies

DISD teachers or administrators may post the following with written parental/guardian and stu­dent approval to the principal:

• Student authored work

• Pictures, audio or video of a student (alone or in a group)

• Student Names

Inappropriate Materials or Language

Profane, abusive, or objectionable language or material may not be used to communicate, nor should materials be accessed which are not in line with the rules of school behavior. A good rule to follow is never view, send, or access materials which you would not want your teachers, par­ents or administrators to see. Should students encounter such material by accident, they should report it to their teacher immediately. Any assumed violation will be reported to the appropriate district administrator and the user’s privilege revoked until the concern of violation is reviewed by the appropriate district administrator.

General Guidelines for Using Technology

1. I understand the DISD Student Code of Conduct applies to electronic interaction, just as it would in any face to face interaction.
2. I understand that passwords are private. I will not allow others to use my account name and password, nor will I use other account names and passwords.
3. I will be polite and use appropriate language in my electronic mail messages, multi-user role-playing and/or virtual learning environments, online postings, and other digital communica­tions with others. I will refrain from using profanity, vulgarities, or any other inappropriate language as determined by school administrators.
4. I will use electronic mail and other means of communications such as blogs, wikis, pod­casting, chat, instant-messaging, discussion boards, and virtual learning environments re­sponsibly. I will not use computers, handheld computers, digital audio players, cell phones, personal digital devices or the Internet to send or post hate or harassing mail, pornography, make discriminatory or derogatory remarks about others, or engage in bullying, harassment, or other antisocial behaviors either at school or at home.
5. I understand that I represent the school district in all my online activities. I understand that what I do on social networking websites such as MySpace and Facebook should not reflect negatively on my fellow students, teachers, or on the District.
6. I understand that masquerading, spoofing, or pretending to be someone else is forbidden.

110

This includes, but is not limited to, sending out e-mail, creating accounts, or posting mes­sages or other online content (e.g. text, images, audio or video) in someone else's name.

7. I will use technology resources responsibly. I will not retrieve, save, or display hate-based, offensive or sexually explicit material. I am responsible for not pursuing material that could be considered offensive. I understand that I am to notify an adult immediately if I encounter materials which violate appropriate use.

8. I will use technology resources productively and responsibly for school-related purposes.

9. I will refrain from attempting to bypass, or circumvent, security settings or Internet filters, or interfere with the operation of the network by installing software or web-based services.

10. I understand that vandalism is prohibited. This includes but is not limited to modifying or destroying equipment, programs, files, or settings on any computer or other technology re­source.

11. I will respect the intellectual property of other users and information providers. I will obey copyright guidelines. I will not plagiarize or use other’s work without proper citation and permission.

12. I will refrain from the use of or access of files, software, or other resources owned by oth­ers without the owner’s permission. I will use only those school network directories that are designated for my use and for the purpose designated by my teacher.

13. I will follow all guidelines set forth by the District and/or my teachers when publishing schoolwork online such as a website, blog, wiki, discussion board, podcasting or video server.

14. I understand the Internet is a source for information that is both true and false and that the school is not responsible for inaccurate information obtained from the Internet.

15. I understand that district and/or campus administrators will deem what conduct is inappropri­ate use if such conduct is not specified in this agreement.

16. I agree to abide by all Internet safety guidelines that are provided by the school and to com­plete all assignments related to Internet safety.

17. I understand that any reported assumed violation of the Student Acceptable Use Policy will be judged by the appropriate district administrator. I also understand that any or all of my privileges may be revoked at any time until the appropriate administrator reviews the concern or violation and makes a ruling.

18. I understand that any dispute involving the Acceptable Use Policy will be settled at the dis­cretion of the school or district administrator that is responsible for student discipline.

Any dispute involving Acceptable Use of district or personal resources will be settled at the dis­cretion of District personnel.

Student AUP Resource Material

APPROVED BOARD POLICY [CQ (LOCAL)]

The Superintendent or designee shall implement, monitor, and evaluate electronic media resourc­es for instructional and administrative purposes.

Access to the District’s electronic communications system, including the Internet, shall be made available to students and employees in accordance with administrative regulations.

Access to the District’s electronic communications system is a privilege, not a right.

All users shall be required to acknowledge receipt and understanding of all administrative regula­tions governing use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations and guidelines may result in suspension

111

or termination of privileges and other disciplinary action consistent with District Policies. [See DH, FNC, CQ, FO, and the Student Code of Conduct]

Violations of law may result in criminal prosecution as well as disciplinary action by the District.

The Superintendent or designee shall develop and implement administrative regulations, guide­lines, and user agreements, consistent with the purposes and mission of the District and with law and policy governing copyright. [See CQ]

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential and may be monitored at any time by desig­nated District staff.

The District shall not be liable for users’ inappropriate use of electronic communication re­sources or violations of copyright restrictions, users’ mistakes or negligence, or costs incurred by users. The District shall not be responsible for ensuring the accuracy or usability of any informa­tion found on the Internet.

Training

Denton ISD will provide training to users in proper use of the system and will provide all users with copies of the Denton ISD Acceptable Use Policy. All Denton ISD training for the system will emphasize its ethical use.

Copyrighted Materials

Copyrighted software of data may not be installed on the system without permission from the holder of the copyright. Only the owner of the copyright (or individuals the owner specifically authorizes in writing) may upload copyrighted material to the system.

Internet Safety

Denton ISD will use technology protection measures to prevent users and students from access­ing pornography or other material deemed harmful to minors. Technology Protection Measures are defined as specific technologies that block or filter Internet access to inappropriate content. Inappropriate content is defined as:

1. Obscene, as defined in section 1460 of title 18, United States Code.
2. Child pornography, as defined in section 2256 of title 18, United States Code.
3. Harmful to minors (including Websites about violence, racism/hate).
4. Disruptive to learning in the classroom (including sites with non-educational games).
5. Inappropriate for minors (including websites that contain hacking instructions, Web email, Adware, Spyware, SPAM Internet fraud and scams and any other areas deemed inappropriate determined by the campus administrator).
6. Harmful to the technology protection measure (including Websites with proxy servers that can be used to bypass the filters).
7. Illegal (including piracy Websites).
8. Personal Web spaces should not identify the user’s relationship to Denton ISD.
9. Controls on the technology protection measures may be updated daily. Sometimes the con­trols may prevent access to sites needed for educational or administrative use. If a user needs to access a blocked site, they may submit a HEAT ticket to have the Website reviewed.

112

Responsibilities

The Superintendent will designate a district-level administrator to:

1. Disseminate and enforce acceptable use policies and guidelines at the district level.
2. Ensure that all users read and sign an agreement to abide by Denton ISD’s policies and guidelines regarding use of the system.
3. Have campus personnel store student signed agreements (electronic or handwritten).
4. Monitor activity on the system (as needed).
5. Establish a retention schedule for messages on any electronic bulletin board.
6. Remove local messages that are inappropriate.
7. Set limits for disk utilization and mailbox sizes on Denton ISD’s system.

Principals will designate campus-level coordinators to:

1. Disseminate and enforce acceptable use policies and guidelines at the campus level.
2. Ensure that teachers adequately supervise their students and are responsible for their stu­dents’ use of the system.
3. Ensure that teachers who supervise students provide training to students that emphasize ap­propriate use of the system.

Cyber-Bullying and Harassment

Threatening, harassing, and/or bullying others using electronic means to include the Internet and/or mobile technology is strictly prohibited.

Vandalism and Abuse

Vandalism is activity that intends to harm or destroy any part of the system, another user’s data, or any agencies or network connected to the Internet or using any means to possess vandalism tools on network drives, pen drives, removable media, or the local computer.

Vandalism includes deliberate attempts to degrade or disrupt system performance. Vandalism includes, but is not limited to,

1. Denials of Service (DOS) attacks
2. Distributed Denial of Service (DDoS) attacks
3. Uploading or creating viruses
4. Using keystroke recording systems
5. Loading Spyware or Adware
6. Using port scanners or other tools to do network reconnaissance
7. IP spoofing
8. Man-in-the-Middle attacks
9. Traffic sniffing
10. Using any other tools to hack into or spy on the system

Vandalism is strictly prohibited and vandals will lose access to the system and must provide res­titution for hardware and software costs associated with system restoration.

Vandals may be prosecuted under applicable state and federal laws.

Denton ISD will cooperate fully with local, state, or federal officials in any investigation con­cerning or relating to vandalism of Denton ISD’s system, any other system or any investigation of misuse.

113

Email Abuse

Attempts to read, delete, copy, or modify the electronic mail of other users or deliberate interfer­ence with the ability of other system users to send/receive email is prohibited. Forgery or at­tempted forgery of email is prohibited.

Plagiarism

Copying any content from the Internet or the system that doesn’t belong to the user and claiming that the content is the property of the user is prohibited. Users must cite the source when includ­ing content from the Internet or the system.

Third Party Content

Users and parents of students with access to the system should be aware that users and students might access other systems in the global network that may contain inaccurate and/or objection­able material.

Any student or employee who brings prohibited materials into the system is subject to suspen­sion, revocation of access, and is subject to disciplinary action in accordance with the Student Code of Conduct.

Revocation of Access

If any user violates the Acceptable use Policy, Denton ISD may suspend the user’s access to the system. Denton ISD will terminate the user’s accounts on the date the principal or Denton ISD administrator receives notice of student withdrawal or revocation of system privileges, or on a future date if specified in the notice.

Disclaimers

System Access: Access to the system is provided on an “as is, available” basis. Denton ISD does not make any warranties with respect to any services provided by the system and about any in­formation or software contained on the system. Denton ISD does not guarantee that the functions or services performed by, or that the information of software contained on the system will meet the user’s requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

User Information: Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system belong to the providers and not Denton ISD.

Liability

Denton ISD is not liable for inappropriate use of Denton ISD’s system or violations of copyright restrictions, mistakes or negligence caused directly or indirectly by users, or costs that users incur. Denton ISD is not responsible for ensuring the accuracy or usability of any information on the Internet.

114